ELSEVIER

network SECURITY

ISSN 1353-4858 October 2018

www.networksecuritynewsletter.com

Featured in this issue:

Be ready to fight new 5G vulnerabilities

We are beginning to see new vulnerabilities open up through 3G and 4G networks, and it is more than likely that 5G will suffer the same fate.

In addition to mitigating and stopping terabit-scale attacks coming from the Internet, it is imperative for enterprises to improve their security by using full-spectrum defences that protect the whole infrastructure. With the assistance of 5G service providers, businesses can then rest easy knowing they have multiple lines of defence, explains Ronald Sens at A10 Networks.

Full story on page 6…

IoT and regulation – striking the right balance

Regulation is certainly one route that can be taken to resolve the serious security challenges posed by the Internet of Things (IoT).

The IoT network has huge potential for businesses to help support cost reduction, streamline operational processes and improve overall service delivery to customers. But the success of the IoT market has caused its security to become a growing concern. However, caution is needed when considering the regulation as it could damage innovation, argues Marco Hogewoning of RIPE NCC.

Full story on page 8…

Love and marriage: why security and SD-WAN need to go together

Thanks to the relentless rise of cloud computing and remote working, the demand for high-bandwidth wide area network (WAN) links over the past few years has never been higher.

The strain on connectivity to the WAN can increase organisations' vulnerability to a cyber-attack. Software-defined WAN (SD-WAN) is a technology that allows organisations to centralise control or intelligently direct their WAN traffic. A security solution that ties into SD-WAN means that organisations can protect their data and ensure that a new approach to networking doesn't mean greater risk, says Marc Sollars of Teneo.

Full story on page 10…

China put spy chips in servers, claims Bloomberg

The Chinese Government has embedded spy chips in servers made by a US company and used by Amazon, Apple, US military and intelligence organisations and many other firms, according to a report by Bloomberg. However, there are few technical details available and the claims have been denied by all the companies named in the article.

According to the story by Jordan Robertson and Michael Riley, high-performance servers made by Silicon Valley firm Super Micro Computer (commonly known as Supermicro) were compromised by having a chip added to each motherboard during manufacture in China. Said to be no bigger than a surface-mount capacitor, it seems these

Continued on page 2…

Contents

NEWS

FEATURES

Editorial Office:
Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.networksecuritynewsletter.com

Publishing Director: Bethan Keall

Editor: Steve Mansfield-Devine
E-mail: infosec@webvivant.com

Senior Editor: Sarah Gordon

Columnists: Tim Erridge, Karen Renaud, Colin Tankard

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/network-security/1353-4858

12987
Digitally Produced by
Mayfield Press (Oxford) Limited

...Continued from front page

chips (there were several versions) were able to contain enough memory and processing capacity to intervene as instructions were routed to the server's processor, via a connection to the baseboard management controller. The implication is that attackers would have a back door into the systems and would be able to remotely inject malware and even malicious firmware.

The report claims that the chips were added to some Supermicro servers that were manufactured by four sub-contractors to the main Chinese fabrication plant. This was under the supervision of members of the People's Liberation Army, who bribed or threatened factory managers, it's alleged.

Both Apple and Amazon, it's claimed, discovered the issue in 2015 – Apple as a result of noticing unusual network traffic and firmware issues and Amazon as part of investigations during the acquisition of Elemental Technologies, which specialises in video streaming. That company's products are used by, among others, Department of Defense datacentres, CIA drone operations and US Navy warships. At around the same time, Apple suddenly cancelled a major order with Supermicro and severed all business with the firm – although Apple claims this is for other reasons.

The Bloomberg story alleges that the firms called in the FBI and that an investigation has been underway ever since.

Apple and Amazon have also issued very strong denials of the story. According to Amazon: "It's untrue that AWS knew about a supply chain compromise, an issue with malicious chips, or hardware modifications when acquiring Elemental. It's also untrue that AWS knew about servers containing malicious chips or modifications in datacentres based in China, or that AWS worked with the FBI to investigate or provide data about malicious hardware." And Apple responded: "On this we can be very clear: Apple has never found malicious chips, 'hardware manipulations' or vulnerabilities purposely planted in any server."

Such specific denials could cause serious regulatory and legal problems for the publicly listed companies if it turns out that they did, in fact, know about compromised servers. And the companies have been backed up by security agencies in the US and UK.

However, if the story is true, it would represent the first major, large-scale compromise of the supply chain at the manufacturing stage. And it has raised awareness of the issue. Thanks to the leaks by Edward Snowden, we know that the NSA was known to intercept equipment during transmit in order to fit backdoor devices, but this was on a small, highly targeted scale.

"Any alleged compromise of the hardware supply chain is a worrying event," said Kurt Baumgartner, principal security researcher at Kaspersky Lab. "Big companies such as Facebook and Amazon design their own hardware because they use so much of it, so it would make sense that they would be the ones to find anything, and it is important that such companies keep examining their platforms. However, sooner or later, the chip would have to phone home and it is when communicating with the attacker's command and control system that undiscovered threats are often most vulnerable. A defender looking at network traffic suddenly spots the anomaly. This is a big problem for threat actors, but it helps the security industry. We and other security companies have warned about a rise in supply chain attacks for a while now and it is an area that organisations need to be very alert to. Even things such as USB sticks still need checking for irregular traffic as they continue to be actively used to spread infection."

All of the sources for the story are unnamed. Following scepticism from the security industry and others, Bloomberg followed up with a second story alleging that a "major US telecommunications company" had recently stripped out servers from Supermicro following the discovery of an implanted chip on the Ethernet interface.

This revelation comes at a time when President Donald Trump and Vice President Mike Pence have both made accusations that China is engaged in cyber-attacks against the US and, in particular, is attempting to meddle in the upcoming mid-term elections. No evidence has been offered to substantiate these claims.

Threatwatch

Banking zero day

Kaspersky Lab says it identified a zero-day exploit (CVE-2018-8453) targeting Windows platforms that was used in targeted attacks against systems in the Middle East. The vulnerability has since been patched. According to Kaspersky, the exploit was delivered to the victims' systems via a PowerShell backdoor. "It was then executed in order to get the necessary privileges for persistence on victim systems. The code of the malware was of high quality and was written to enable the reliable exploitation of as many different Windows builds as possible," the firm said. There's more information here: http://bit.ly/2A4v62V.

Most sophisticated botnet

Researchers at Avast have released details of Torii, which they are calling the most sophisticated Internet of Things (IoT) botnet seen to date. While there have been many variants of Mirai, this new botnet distinguishes itself through its advanced techniques. It spreads via unsecured telnet connections via Tor exit nodes. And unlike Mirai and its many spin-offs, Torii doesn't engage in distributed denial of service (DDoS) or crypto-jacking. Instead, it has, says Avast, "a quite rich set of features for exfiltration of (sensitive) information, modular architecture capable of fetching and executing other commands and executables and all of it via multiple layers of encrypted communication." There's more information here: http://bit.ly/2pOSknH.

Magecart strikes again

The Magecart exploitation kit, which is designed to produce exploits for e-commerce sites, has claimed another victim. According to RiskIQ, which has been tracking the malware, malicious JavaScript has been inserted into the Shopper Approved plugin, which is used on a large number of sites to allow customers to leave reviews. It's possible that the people behind this attack are the same ones that inserted Magecart code into Feedify a month ago. Both attacks made use of the same server for exfiltrating data. Magecart was also implicated in the breaches at British Airways and Ticketmaster. There's more information here: http://bit.ly/2A2BZBI.

Betabot is back

Security firm Cybereason says it has seen a batch of infections by the Betabot (aka Neurevt) malware. The information-stealing malware, which started life as a banking trojan back in 2012, has gained new features and can "practically take over a victim's machine and steal sensitive information," says Cybereason. The main vulnerability exploited by the malware is an 18 year-old flaw in the Equation Editor tool in Microsoft Office. The vulnerability has been around since the tool's introduction in 2000, but was publicly discovered by researchers – and patched by Microsoft – only in 2017. There's more information here: http://bit.ly/2NyzOt5.

Panda update

The Panda Banker trojan, first seen in 2016, has received a number of updates and is highly active in the US, Canada and Japan, according to Cylance. It exploits man-in-the-browser techniques to inject code into web pages viewed by the victim. This code is used to steal bank, payment card and personal information. Recently, Cylance has seen it being delivered by the Emotet exploit kit. According to the firm: "Heavy code obfuscation and multi-encryption layering make it difficult to dissect this malware's C2 communication and malicious scripting." There's more information here: http://bit.ly/2CbitVg.

China manufactures around 90% of the world's PCs and 75% of the world's mobile phones.

The Bloomberg story is here: https://bloom.bg/2E7RE6C.

Flaw leads to Google+ shutting down

A vulnerability that made profile information for 500,000 or more Google+ users potentially open to harvesting has prompted the company to shut down the social networking platform.

The flaw allowed developers of apps that use Google+ as an authentication method to collect profile data on users that had been designated as private. The company discovered the problem in March, but decided to keep it secret as it could find no evidence of the vulnerability having been abused, although it admits there is no definite way of telling.

At the time, social media platforms were under heavy scrutiny, including congressional hearings (which Google refused to attend). An internal memo by Google's internal legal counsel, seen by the Wall Street Journal, recommended non-disclosure because doing otherwise would be likely to result in "immediate regulatory interest".

The bug was found as part of an API review called Project Strobe and Google believes it was fixed before anyone else had discovered it.

The firm came to the conclusion that the nature of the vulnerability did not meet the requirements for mandatory disclosure, in spite of the fact that it had been in place from 2015 until it was fixed in March 2018. This is based on the assertion that it had not been exploited. If it had, it would only have exposed "name, email address, occupation, gender and age," according to Google engineering VP Ben Smith. Nevertheless, Google's own Project Zero security team often criticises other firms for non-disclosure even where no breaches occurred.

"Unlike the recent Facebook breach, this disclosure timeline is incomprehensibly long and will likely provoke a lot of questions from regulatory authorities," said Ilia Kolochenko, CEO at High-Tech Bridge. "Inability to assess and quantify the users impacted does not exempt from disclosure. Although a security vulnerability per se does not automatically trigger the disclosure duty, in this case it seems that Google has some reasonable doubts that the flaw could have been exploited. Further clarification from Google and technical details of the incident would certainly be helpful to restore confidence and trust among its users currently abandoned in darkness."

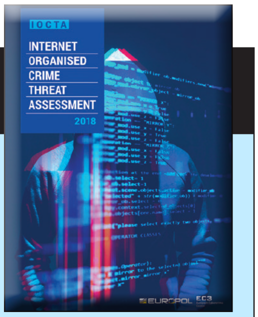
Google's own take on the flaw is here: http://bit.ly/2OMeq8d.

Google+, launched in 2011, never gained the popularity of other platforms such as Facebook or Twitter and it's possible that the company was looking for an excuse to shutter it – Google has a history of launching and then closing platforms.

Google has now announced that it is greatly reducing the amount of user data it shares with third-party developers. There's more information on that here: http://bit.ly/2A2gWzj.

Ironically, this story broke at the same time that Google opened its Google Safety Centre (https://safety.google/) with the home page headline of: "Making technology for everyone means protecting everyone who uses it." The service aims to inform users about how Google keeps their personal information safe and provides links to privacy controls.

Report Analysis



Europol: Internet Organised Crime Threat Assessment

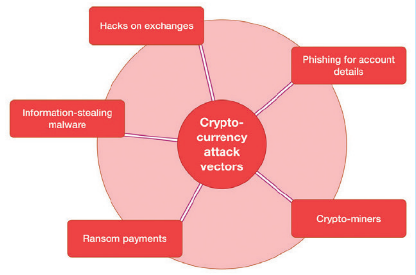
Europol's fifth edition of its annual Internet Organised Crime Threat Assessment (IOCTA) report presents a dark picture – one in which current cybercrime activity continues largely unabated while being joined by innovative new ways for the criminally minded to exploit the Internet for illicit gain. At the same time, technological and regulatory changes have made life harder for law enforcement.

As an example of the latter, the General Data Protection Regulation (GDPR) has resulted in names and contact information being removed from publicly accessible WHOIS data. This makes it difficult for security researchers and (to a slightly lesser extent) law enforcement agencies to see who owns specific domains.

"GDPR, while increasing privacy for normal users has also enhanced criminals' ability to hide their identity and activity," commented Ross Rustici, senior director at Cybereason. "Additionally, the increased cases of cyber-extortion can be directly linked to the fines laid out in the new law. Despite the best intentions, the EU incidentally increased the profitability and immunity of cyber-criminal activity. That is a price they may be willing to pay, but it has a significant negative effect on those attempting to discover and disrupt cyber-criminal behaviour."

New 5G mobile networks also pose problems for law enforcement. The ability to dynamically switch and merge traffic from multiple networks – including wifi, cellular and satellite – makes it difficult to perform lawful interception or monitoring of specific communications. In addition, while 4G technology assigns permanent identifiers to each mobile device, 5G employs temporary IDs, making tracking much harder.

Among the continuing issues noted over the past year, Europol cites ransomware, distributed denial of service (DDoS) attacks, card-not-present fraud and social engineering (including phishing) as persistent threats. While most reports show ransomware slowing down, Europol reckons it is overtaking banking trojans as the chief form of financially motivated malware. The report also notes the increased use of ransomware by nation-state actors: WannaCry, for example, is now widely blamed on North Korea and it seems to have been used as a data destruction tool rather than any serious attempt to reap financial rewards.


Hacks on exchanges
Phishing for account details
Information-stealing malware
Crypto-currency attack vectors
Crypto-miners
Ransom payments

Issues associated with crypto-currencies.

The use of exploit kits has declined, which might suggest a win for defences such as anti-malware, better patching and so on. The truth may be less encouraging, however. Exploit kits are still in widespread use, with their main focus having shifted from ransomware to crypto-mining. However, cyber-criminals now seem more interested in using less technically demanding vectors to achieve infections, such as spam and phishing.

One worrying trend highlighted by Europol is the increase in child sexual exploitation material (CSEM) being found online, including so-called self-generated explicit material (SGEM), much of it generated and shared via social media platforms. Children's ready access to the Internet, the development of technologies such as live streaming and issues of jurisdiction make this a challenging problem to police. P2P platforms remain the chief means of sharing CSEM, but the report also notes the increased use of the dark web.

One of the thorniest issues for law enforcement is the increasing popularity, among both law-abiding and criminal communities, of crypto-currencies. The past few years have seen systems such as Bitcoin and Monero move into the mainstream, with the currencies being accepted by respectable online businesses and an increasing number of ordinary users turning to them.

At the same time, criminals continue to make use of the anonymous nature of crypto-currency transactions to pay the bills for their activities (such as server or botnet rentals), cash-out on malware or fraud campaigns, launder funds from illegal activity and receive payments from victims targeted with ransomware attacks or extortion. On top of that, we can now add a new form of criminal activity that is rapidly rising in popularity – crypto-jacking – in which the power of victims' machines is harnessed to mine crypto-currencies. And crypto-currency exchanges have come under frequent attacks, with millions of dollars' worth of currency being stolen.

One of the rare success stories in the cybercrime world in the past couple of years has been the taking down of so-called 'darknet' markets. In 2017, co-operative policing efforts between the FBI, the US Drug Enforcement Agency (DEA) and the Dutch National Police, with Europol, other law enforcement bodies and security firms in support, dismantled two of the largest markets on the dark web – AlphaBay and Hansa. Along with the Russian Anonymous Marketplace (RAMP) – shut down by Russian authorities in July 2017 – these accounted for 87% of darknet market trade.

"Collaboration appears to be one of the biggest and most prominent takeaways. Being able to establish trustworthy channels to collaborate and share information and intelligence is vital," commented Javvad Malik, security advocate at AlienVault.

It's not quite the victory it sounds, though. Numerous other, smaller markets have sprung up to take their place, mostly selling drugs.

There are certain methodologies and technologies that cut across many types of cybercrime, but some are finding new use cases. Phishing remains the primary social engineering vector and is rapidly climbing in volume. It is also the foundation of one of the fastest-growing forms of fraud – business email compromise (BEC) – which is being enthusiastically adopted by West African fraudsters.

The report is available here: www.europol.europa.eu/Internet-organised-crime-threat-assessment-2018.

In brief

Vulnerable weapons

Nearly all US military weapons systems developed in the period 2012 to 2017 contain vulnerabilities to cyber-attack, according to an investigation and report by the Government Accountability Office (GAO). In penetration tests, researchers were able to hack into some of these complex weapons systems and take control over them "using relatively simple tools and techniques". According to a GAO announcement: "The Department of Defense (DOD) faces mounting challenges in protecting its weapon systems from increasingly sophisticated cyber threats. This state is due to the computerised nature of weapon systems; DOD's late start in prioritising weapon systems cyber security; and DOD's nascent understanding of how to develop more secure weapon systems. DOD weapon systems are more software dependent and more networked than ever before." The report is available here: www.gao.gov/products/GAO-19-128.

Dodgy devices

Chinese manufacturer Xiongmai is in the firing line again for selling Internet-connected devices that are vulnerable to attack. DVRs and IP cameras made by Xiongmai (aka Hangzhou Xiongmai Technology) were one of the main targets in the Mirai botnet outbreak, mainly because of the vendor's habit of distributing devices with weak, or missing, login credentials. Although the two other manufacturers implicated in that incident – Huawei and Dahua – have taken steps to improve the security of their products, Xiongmai has refused to do so, even after months of working with Austrian security firm SEC Consult.

Having become frustrated with Xiongmai's intransigence, SEC Consult has halted work with the firm and has released a report detailing multiple failings. Most of these relate to the XMEye peer-to-peer (P2P) communications solution that is included in all Xiongmai devices and allows them to connect to a cloud service. This makes the devices accessible from anywhere in the world via an easily-guessable unique ID (UID), usually tied to the device's MAC address. While XMEye requires a username and password, in many products the default username is 'admin' and the password is blank. This gives full access to the device. Some devices offer slightly limited access using the username of 'default' and the password 'tluafed' (default backwards). Although login credentials can be changed, many users will leave the default ones in place. SEC Consult calculates there are around 9 million Xiongmai P2P devices connected worldwide, nearly all of them sold under other brand names. There's more information here: http://bit.ly/2C7Kg8X.

California bans weak passwords

California has just passed state law making it illegal to sell Internet-connected products, such as Internet of Things (IoT) devices, that have default passwords that are easy to crack. The law comes into effect in 2020, and while it will affect only products sold in the state, some are seeing it as a 'best practice' guideline for wider adoption. A federal bipartisan bill, the 'Internet of Things Cyber-security Improvement Act', introduced in the wake of the Mirai attack, is still clawing its way through the Senate with no guarantee of survival. The 'Information Privacy: Connected Devices' bill is here: http://bit.ly/2pMDNso.

Breached records hit new high

In the first six months of 2018, 4.5 billion records were compromised in cyber-breaches, according to Gemalto's latest 'Breach Level Index'. This is a 133% increase over the same period in 2017. A total of six social media breaches, including the Cambridge Analytica/Facebook incident, accounted for over 56% of total records compromised. Of the 945 data breaches, 189 (20% of all breaches) had an unknown or unaccounted-for number of compromised data records. The US was most affected, with 540 breaches and 3.25 billion records affected – an increase of 98%. The UK had 22 breaches during the six months, a 51% drop, with only 39,375 records affected. Government organisations accounted for 27% of UK breaches, followed by education (18%) and healthcare (18%). And nearly half (45%) of the records were affected by accidental loss, rather than cyber-attacks. There's more information here: https://breachlevelindex.com/.

NHS refuses to invest in security

The UK's National Health Service (NHS) is likely to ignore the recommendations of a government-commissioned report by its own CIO, Will Smart, that calls for an investment of £800m-£1bn in cyber-security. The review that resulted in the report was started in the wake of the WannaCry ransomware that affected multiple NHS organisations. And it also found that the NHS is under constant attack by malware, including Orangeworm, which "specifically targets sensitive healthcare data" and has been attacking the NHS for some time. There have been notable exploits of medical devices and 80% of NHS trusts failed to respond to a high-severity cyber alert in April. Yet NHS Digital is believed to be reluctant to follow the recommendations of Smart's report because of the high costs. Responding to inquiries from the Health Service Journal, the Department for Health and Social Care stated: "The health service has improved its cyber-security since the attack and we have supported this work by investing over £60 million to address key cyber-security weaknesses. We plan to spend a further £150 million over the next two years."

Twitter safeguards elections

Ahead of the US mid-term elections, Twitter has announced that it has boosted detection capabilities aimed at weeding out fake accounts and has also beefed up its enforcement policies. VP of truth and safety, Del Harvey, and head of site integrity, Yoel Roth, wrote in a blog post that the steps were part of an 'election integrity' programme. Key signs that an account might be fake, they explained, are the use of stock or stolen avatar images, stolen or copied profile information and misleading profile data, such as location. And while banned users can simply open new accounts, Twitter is watching out for accounts that "deliberately mimic or are intended to replace accounts we have previously suspended for violating our rules". The tougher stance and automated detection rules have resulted in 9.4 million accounts being queried each week in the first half of September, which also led to a slight drop in user-reported spam. There's more information here: http://bit.ly/2CBtP5Q.

Vulnerable networks

More than two-thirds of organisations believe that their networks are vulnerable to attacks by hackers, according to new research by Radware. The firm found that 89% of organisations have suffered an application layer attack in the past year and many are coming under weekly or even daily attack. Some 70% of businesses have unsecured third-party APIs. More than third (35%) of companies are losing customers because of data breaches and 23% have fired IT executives as a result. The report is available here: http://bit.ly/2Ofxbl2.

CORRECTION

In the article, 'Is quantum computing becoming relevant to cyber-security?' in the September issue of Network Security, there was a character translation problem with some special characters in the box copy on pg.18. The last section of the copy should have read:

Another common notation in quantum programming is the famous bra-ket notation, named after the symbols: bra, $\langle x|$, and ket, $|y\rangle$. Nominally, each represents a quantum state vector. For example, a single qubit has two possible states, $|1\rangle=(0,1)$ and $|0\rangle=(1,0)$. Further, it can exist in a superposition of both states, $|\varphi\rangle = a|1\rangle + b|0\rangle$. The qubit is, by definition, a normalised vector, which we represent by taking the inner product of the qubit's state with its complex conjugate, such that:

$\langle\varphi|\varphi\rangle = 1$,

which evaluates to $|a|2 + |b|2 = 1$. Once the state of the qubit is 'observed' and the wave function collapses, it resolves to either 1 (with probability $|a|2$) or 0 (with probability $|b|2$).

Be ready to fight new 5G vulnerabilities

Ronald Sens

Ronald Sens, A10 Networks

In the evolving landscape of mobile networks, we are beginning to see new vulnerabilities open up through 3G and 4G networks, and it is more than likely that 5G will follow this same fate. Protecting only this Gi Interface is no longer enough for any service providers' security.

Until recently, the Gi-LAN connecting the EPC (Evolved Packet Core) to the Internet was considered to be the most vulnerable part of the service provider network and was protected via Gi-Firewall and anti-DDoS systems. The rest of the EPC links were considered difficult targets for hackers because advanced vendor-specific knowledge was required for a successful attack. Since the typical hacker prefers a soft target, defensive measures weren't a priority for developers or carriers. Network complexity was a defence in itself.

However, the requisite know-how to attack EPC from other interfaces is now becoming much more common. The mobile endpoints are being infected at an alarming rate and this means that attacks can come from the inside of the network. The year 2016 saw a leap in malware attacks, including headline-makers Gooligan, Pegasus and Viking Horde.[1-3] Then the first quarter of 2017 saw a leap in mobile ransomware attacks, which grew by 250%.

The need for securing the EPC is tied to advances like long-term evolution (LTE) adoption and the rise of IoT, which are still gaining speed. LTE networks grew to 647 commercial networks in 2017, with another 700 expected to launch this year.[4] With the adoption of LTE, IoT has become a reality – and a significant revenue stream for enterprises, creating a market expected to reach £400bn by 2022.[5] The time to take a holistic approach to securing the service provider networks has arrived.

There are three primary data paths connecting mobile service providers to the outside world. The first of these is a link to the Internet through S/Gi LAN. Next is a link to a partner network that serves roaming users. Last, there is a link for traffic coming from towers. The security challenges and the attack vectors are different on each link. Until recently, the link to the Internet was the most vulnerable point of connectivity. DDoS attacks frequently targeted the service provider's core network on the Gi Link. These attacks were generally volumetric in nature and were relatively easy to block with highly scalable firewalls and DDoS mitigation systems.

Expanding attack surface

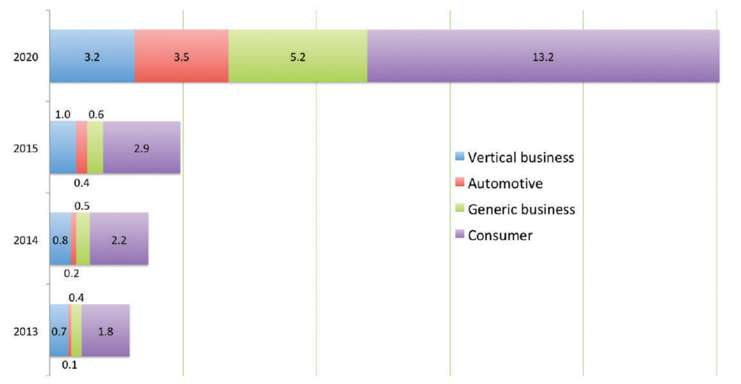
The threat landscape is rapidly changing and attacks can come from other points of connectivity. This has been theoretical until recently; while numerous academic research papers have been published in the past decade suggesting that attacks from partner networks or radio access networks (RANs) were a possibility, those threats are no longer merely an intellectual exercise – they are real. At the same time, the rapid rise of IoT is exposing the threat of malicious actors taking control and weaponising devices against a service provider.

Multiple botnets, such as WireX and its variants, have been found and taken down.[6] So far, these attacks have targeted hosts on the Internet, but it's just a matter of time until they start attacking EPC components. There are multiple weak points in EPC and its key components. These components, which used to be hidden behind proprietary and obscure protocols, now reside on IP, UDP or SCTP, which can be taken down using simple denial of service attacks.

The attack surface is significantly larger than it used to be and legacy approaches to security will not work. A DDoS attack, such as a signalling storm, against an individual entity can be generated by a malicious actor or even a legitimate source. For example, a misbehaving protocol stack in an IoT device can cause an outage by generating a signalling storm.

Defend networks

There are currently 6.8 billion mobile devices in use and innumerable IoT devices. As 5G matures, the number of those types of devices will swell even further – and so will the number and scale of attacks against service providers. The Mirai botnet brought down one site using 300,000 to 500,000 devices to overwhelm one site with 600Gbps of traffic.[7] That was one of the first massive-scale botnet attacks we've seen, but it won't be the last. Attacks that used to take minutes to bring down a network will soon only take seconds.



The growth of the Internet of Things, measured in billions of IoT units installed. Sources: Gartner Symposium/ ITxpo; A.T. Kearney analysis.

While enterprise IT professionals need to be ready to fight back against newly generated threats created through 5G vulnerabilities, the security teams should not be fighting alone. Service providers are eager to know how they can protect their subscribers and their networks from these rapidly evolving and fast-moving threats. Many attendees of the recent IEEE 5G World Forum were adamant that service providers shouldn't count on the manufacturers of IoT devices to build proper security into their products: service providers must take proactive steps to defend their networks and their customers.[8] And these service providers are listening.

EE and BT previously announced their plans to be the first 5G service provider in the UK and announced a test run for October 2018 that is designed to ensure that 5G is ready for public use. They recently went into more details around the steps they will be taking to do this, making it live in 10 specific locations around London and to select users that they can monitor.[9] By undertaking controlled, live, tests they can easily isolate any security vulnerabilities that may crop up and create solutions in advance of the official launching.

While EE has yet to give any direct, technical details for how it plans to fight back against 5G threats, there are several options available to it and other service providers. High-performance stateful firewalls that deliver up to 220Gbps of throughput while supporting up to 256 million concurrent sessions can help to block out and destroy malicious attackers through a 5G network. Meanwhile advanced server load balancing and FPGA-based Flexible Traffic Acceleration (FTA) mitigates common anomaly attacks before burdening CPUs for DCFW functionality. With this, the scale of attacks can be treated without overburdening security tools and teams utilised by these service providers.

Securing the SP network

To secure the SP network, businesses must improve their defences against DDoS attacks. The best way to achieve this is by utilising an S/Gi firewall solution and a DDoS mitigation solution. Threat protection systems (TPS) should also be deployed in your enterprise's IT security on-premise and cloud infrastructures. With all of these solutions in place it becomes easier to mitigate multi-terabit attacks.

Utilising powerful tools that can improve these defences, can help detect and mitigate, or stop, a number of advanced attacks specifically against EPC. The tools being used should also allow for a granular deep packet inspection to protect against user impersonation by means of spoofing, network impersonation and signalling attacks to security professionals.

To summarise, in addition to mitigating and stopping terabit-scale attacks coming from the Internet and utilising stateful firewall services, it is imperative for enterprises to improve their security measures by using full-spectrum security that protects the whole infrastructure of the business. Then with the assistance of 5G service providers, working on their own security measures to help combat malicious attacks through the network, businesses can rest easy knowing they have multiple lines of defence prepared to tackle the onslaught of new vulnerabilities that 5G will undoubtedly bring with them.

About the author

Ronald Sens is EMEA director at A10 Networks and a B2B technology leader and a marketing professional with 20-plus years of technology industry experience in multiple international marketing disciplines. His main areas of expertise are in enterprise mobility, data security and compliance, datacentre, networks, servers and storage, end-user computing, SaaS, virtualisation, enterprise software, mainframe and Unix, and professional and managed services.

References

1. Brewster, Andrew. 'Android 'Gooligan' hackers just scored the biggest ever theft of Google accounts'. Forbes, 30 Nov 2016. Accessed Oct 2018. www.forbes.com/sites/thomasbrewster/2016/11/30/gooligan-android-malware-1m-google-account-breaches-check-point-finds/#720f6c931ad8.
2. Heller, Michael. 'Pegasus iOS exploit uses three zero days to attack high-value targets'. TechTarget SearchSecurity, 29 Aug 2016. Accessed Oct 2018. http://searchsecurity.techtarget.com/news/450303267/Pegasus-iOS-exploit-uses-three-zero-days-to-attack-high-value-targets.
3. Whitney, Lance. 'Viking Horde malware attacks Android devices'. CNet, 10 May 2016. Accessed Oct 2018. www.cnet.com/news/viking-horde-malware-attacks-android-devices/.
4. Dudley, William. '2018 Mobile industry predictions'. Digitalist, 12 Jan 2018. Accessed Oct 2018. www.digitalistmag.com/digital-economy/2018/01/12/2018-mobile-industry-predictions-05728414.
5. 'The Internet of Things (IoT) market is expected to grow from USD 170.57 billion in 2017 to USD 561.04 billion by 2022, at a Compound Annual Growth Rate (CAGR) of 26.9%'. Cision, 22 Jan 2018. Accessed Oct 2018. www.prnewswire.com/news-releases/the-internet-of-things-iot-market-is-expected-to-grow-from-usd-17057-billion-in-2017-to-usd-56104-billion-by-2022-at-a-compound-annual-growth-rate-cagr-of-269-300585814.html.
6. Pascucci, Matthew. 'WireX botnet: How did it use infected Android apps?' TechTarget SearchSecurity, Nov 2017. Accessed Oct 2018. http://searchsecurity.techtarget.com/answer/WireX-botnet-How-did-it-use-infected-Android-apps.
7. 'Investigating Mirai'. A10 Networks. Accessed Oct 2018. www.a10networks.com/resources/white-papers/investigating-mirai.
8. IEEE 5G World Forum, home page. Accessed Oct 2018. http://ieee-wf-5g.org.
9. Snelling, David. 'EE 5G speed boost - Why you'll soon be able to download content over 10 times faster'. Sunday Express, 24 Jun 2018. Accessed Oct 2018. www.express.co.uk/life-style/science-technology/970013/EE-5G-speed-UK-trails.

IoT and regulation – striking the right balance

Marco Hogewoning

Marco Hogewoning, RIPE NCC

The UK Government has made the welcome announcement that it will establish a new Internet of Things (IoT) code of practice – 'Secure by Design' – to increase the security of connected devices.[1] Understandably, this has sparked discussions about whether the code of practice is a precursor to more formal regulation of the IoT. Regulation is certainly one route that can be taken to resolve the serious security challenges that the IoT faces. However, caution should be exercised when pondering the regulation of IoT, as it could serve only to damage IoT innovation and dynamism, threatening the very market growth that it is driving.

The IoT network has huge potential for businesses to help support cost reduction, streamline operational processes and improve overall service delivery to customers. Indeed, the IoT has the potential to generate £8.2tn per year in economic value by 2025, according to data from McKinsey. However, the IoT still faces major security challenges and many businesses might not have a full grasp of the risk posed by this dramatic increase in connected systems. There is genuine confusion over how best to tackle the problem of IoT security. Moreover, who has the actual ethical obligation to protect IoT devices?

Facing the issue

Governments, manufacturers and other stakeholders in the IoT ecosystem must face this issue together, but in such a way that any regulatory framework employed does not hinder IoT market innovation, dynamism and competition.

Strangely, the very success of the IoT market has partly caused its security to become a growing problem. Connected devices have becoming increasingly popular among consumers, which has seen some manufacturers focus purely on getting their products to market more quickly than their competitors. Commercial pressures possibly have led to an environment where some manufacturers are deprioritising product security, to gain that valuable first-to-market advantage. Another reason for this could be that many of these manufacturers are new to developing connected devices, so they just don't have the technical expertise on how to keep these products secure. Whichever one it is, it's deeply worrying and could have grave consequences.

> ***"In a post-Mirai world, many analysts close to the issue are concerned about a sort of malware 'time bomb' – with the full extent of such an attack only realised after the fact"***

Just consider the destructive Mirai botnet attack of October 2016, in which large numbers of IoT devices were infected with malware.[2] Or, more recently in January 2018, when a 'Mirai-variant' (which exhibited self-propagating capacity) was believed to have played a part in a string of cyber-attacks instigated against various Fortune 500 financial businesses.[3] More worrying still, is the prospect of a Reaper-sized botnet attack and the impact such an attack might have upon the Internet.[4] In a post-Mirai world, many analysts close to the issue are concerned about a sort of malware 'time bomb' – with the full extent of such an attack only realised after the fact. Because of the vulnerabilities that continue to plague devices within the IoT space, the prospect of zombie connected devices quietly wreaking havoc upon the Internet remains a real threat for many commentators.

Cyber incursions such as Mirai and the subsequent looming threat of a Reaper botnet attack, have served to underline the serious consequences of lax IoT device security. However, the approach that certain manufacturers take is not the only problem. There is also the question of which party is actually responsible for protecting IoT devices from cyber threats.

Most connected devices remain active, through occasional updates and patches, for years – even decades. IoT devices also tend to not have a user interface, so there is a big question mark around how to notify end-users when security updates are available. Usually, if a product meets current standards and the conditions of its guarantee, it stops becoming the responsibility of the manufacturer upon sale. However, connected devices are totally different. As the threat landscape keeps evolving and new vulnerabilities are found on an almost daily basis, manufacturers need to make sure updates are made available on a going-concern basis. Additionally, the owners or operators of these devices must also ensure that those updates are actually installed on the device.

The challenge ahead

This is a challenging situation, one that – if we're to address it effectively – will certainly require a good degree of open dialogue and discussion among the increasing number of stakeholders within the IoT. Yet, this challenge is only exacerbated by the fact that incentives towards co-operation, especially when it comes to sharing experiences, are notably absent from the IoT ecosystem.

The need for interconnection and interoperability means that competing

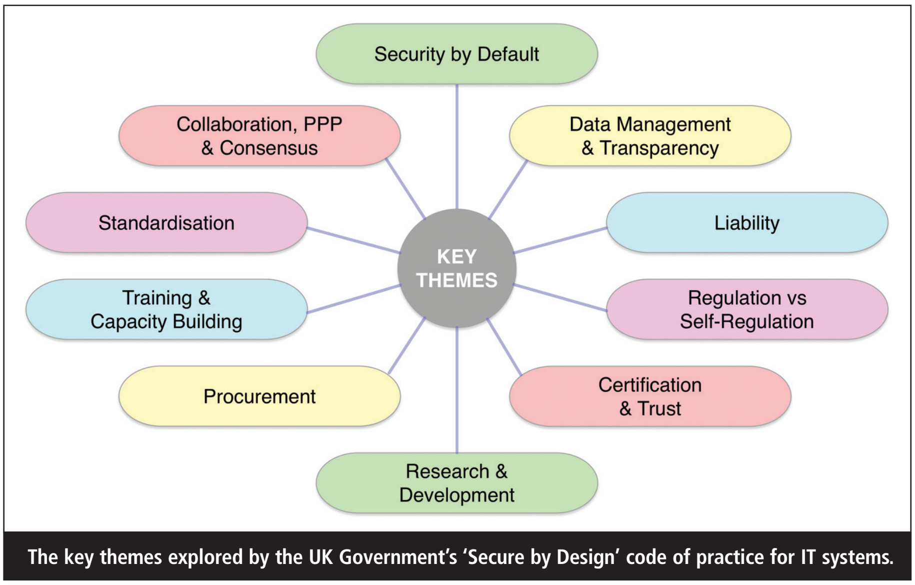
Internet companies have always had a strong incentive to co-operate in certain areas. Over time, this led to the growth of technical communities that regularly meet to share experiences and develop best practices that contribute to a more secure and robust Internet. Unfortunately, IoT developers are usually working in isolation from one another, which leads to their reinventing the wheel when they look to develop safe and secure products – with little in the way of best practices to guide them.

With these challenges considered, we can begin to understand some of the parameters that we must work around when answering the question of what exactly a workable solution looks like. Through understanding such obstacles, we're better placed to examine the possible merits and drawbacks of particular solutions, and why the most obvious answers – like regulation – might not necessarily be the most viable.

The progress we've seen

It is certainly encouraging that strides are being made towards ensuring that IoT applications and devices are more secure. One example of these efforts is the UK Government's IoT code of practice. In March 2018, the Department for Digital, Culture, Media & Sport (DCMS) revealed this guidance (along with an accompanying literature review) with a view to boosting IoT security. Any measures that push all stakeholders to better understand their role in IoT security – and take it very seriously – are very welcome. However, formal regulation of the IoT could end up not having the desired outcome and actually harm the IoT marketplace.

Enforced regulation around IoT security could impact innovation and damage the dynamism and competition that has seen the network grow and drive real benefits. For example, suppose a government decides to establish a single regulator to oversee the IoT. Setting up such a body would, in the first instance, be genuinely challenging as it would need to include such a very diverse array of capabilities. Running such an operation would be even harder, as it would also need to traverse the many different sectors in which IoT devices are leveraged. Such complications in founding, and maintaining, a body like this could result in regulation that is not fit for purpose for a particular IoT vertical. The knock-on effect of this could be that the vibrancy of the IoT market suffers.


KEY THEMES
Security by Default
Collaboration, PPP & Consensus
Data Management & Transparency
Standardisation
Liability
Training & Capacity Building
Regulation vs Self-Regulation
Procurement
Certification & Trust
Research & Development

The key themes explored by the UK Government's 'Secure by Design' code of practice for IT systems.

"Everyone could work towards being more secure in the development of IoT devices, but also enjoy healthy competition to maintain the successful and dynamic status of the market"

If a single regulator is tricky, a sectoral approach to IoT security could be employed. This would involve existing industry regulators co-operating with IoT stakeholders to discuss shared values and opening a path to voluntary IoT security standards. A collaborative and open approach works. After all, the Internet was founded on an approach like this.

The self-regulation of the IoT space by its own stakeholders could be a great route to establishing best security practice and processes, but without impinging on the innovation in the IoT space. Everyone could work towards being more secure in the development of IoT devices, but also enjoy healthy competition to maintain the successful and dynamic status of the market. For example, the DCMS directly collaborated with a range of manufacturers, retailers and government bodies to agree to the IoT code of practice.

A collaborative solution

This co-operative strategy, built around establishing and continuing debate between stakeholders, promotes openness and could deliver the valuable security standards the IoT network desperately requires. With voluntarily agreed standards being adopted for the IoT, manufacturers, and others, can feel free to innovate and compete – but also to design products which are centred around robust security.

Established and open communities from the 'traditional' Internet industry, who have been working on these issues for decades, including the RIPE NCC, the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE) and Worldwide Web Consortium (W3C), among others, can support government organisations and manufacturers in coming to terms with the world of the IoT. Working with these open organisations can be hugely beneficial to knowledge sharing, best practices and the kind of healthy debate around the norms – and expected behaviour – of IoT devices.

This clear and collaborative process has served the Internet industry very well, and could do the same for the IoT – resulting in much more resilient devices for consumers. This is something that really matters, but there is still some way to go until it is seriously addressed in the IoT world. It is encouraging to see collaborative initiatives around IoT security being launched into the market. Vigorous debate is the first step in establishing the voluntary IoT security standards that could see the network thrive.

> *"It is crucial that businesses operating in the IoT, either now or in the future, put market pressures to one side when thinking about, and working to solve, the challenges they face in making the IoT safer for end users"*

However, a genuine change in mindset is also required. Commercial pressures and objectives are clearly important to manufacturers and every organisation in the IoT space, but these must be considered even-handedly with keeping the network secure. This is an objective that every interested party needs to work towards. The IoT offers huge benefits to businesses and society as a whole, but in order for this huge opportunity to be grasped it requires a unique and all-encompassing security framework.

Whatever a solution looks like, open discourse will be a key component. For this dynamic to be achieved, it is crucial that businesses operating in the IoT, either now or in the future, put market pressures to one side when thinking about, and working to solve, the challenges they face in making the IoT safer for end users. Any standards need not be enforced (in fact, as outlined throughout this piece, such enforcement would likely prove counterproductive), but nonetheless remain essential. Trust and open discussion will prove to be the crucial ingredients in making the IoT ecosystem safe for all.

About the author

Marco Hogewoning is a senior external relations officer at the RIPE NCC. As part of the External Relations team, he helps lead the RIPE NCC's engagement with its membership, the RIPE community, government, law enforcement and other Internet stakeholders. He joined the RIPE NCC in 2011. Prior to that, he worked as a network engineer for various Dutch Internet service providers and was formerly chair of the RIPE IPv6 Working Group.

References

1. 'Secure by Design'. Department for Digital, Culture, Media & Sport, UK Government, 7 Mar 2018. Accessed Oct 2018. www.gov.uk/government/publications/secure-by-design.
2. 'Mirai (malware)'. Wikipedia. Accessed Oct 2018. https://en.wikipedia.org/wiki/Mirai_(malware).
3. DeNisco Rayome, Alison. 'Mirai variant botnet launches IoT DDoS attacks on financial sector'. TechRepublic, 5 Apr 2018. Accessed Oct 2018. www.techrepublic.com/article/mirai-variant-botnet-launches-iot-ddos-attacks-on-financial-sector/.
4. Whittaker, Jack. 'Fear the Reaper? Experts reassess the botnet's size and firepower'. ZDNet, 30 Oct 2017. Accessed Oct 2018. www.zdnet.com/article/reaper-botnet-experts-reassess-size-and-firepower/.

Love and marriage: why security and SD-WAN need to go together

Marc Sollars

Marc Sollars, Teneo

Thanks to the relentless rise of cloud computing and remote working, the demand for high-bandwidth wide area network (WAN) links over the past few years has never been so high. Analyst firm Forrester predicts that the public cloud market will grow to $236bn by 2020, increasing by 23% in six years.[1] A growth in the use of cloud applications to suit the needs of a mobile workforce has meant that WAN pipes have filled up enormously. Not only that, with companies seeking greater agility and local office autonomy, there is far greater demand to connect work apps to the WAN. All of these factors are putting a strain on organisations and their WANs, and sparking security concerns.

The strain on connectivity to the WAN, whether it's through Multiprotocol Label Switching (MPLS), Internet or 4G, can increase organisations' vulnerability to a cyber-attack, particularly as senior staff members and network users may move almost hourly between different workplace devices. The sheer number of network endpoints now available gives hackers a far greater choice of potential attack-points on corporate networks, evidenced by IDC, which found that 70% of successful breaches originate on the endpoint.[2] The need for ensuring safer WAN connections has never been greater, given this explosion of endpoints. But instead of simply investing in a new firewall to keep data protected, organisations should think bigger when protecting their ever-growing WAN.

Centralised control

Software-defined WAN (SD-WAN) is a technology that allows organisations to centralise control or intelligently direct their WAN traffic. Often deployed as a virtual overlay on top of an existing network, SD-WAN abstracts traffic from underlying private or public WAN infrastructures, such as MPLS and Internet broadband, to enable central IT teams to use multiple 'tunnels' for more effective data transfer and application performance options.

This rise of smart software-defined control techniques, from datacentres and networks, and now in WANs has changed the game, with analyst IDC predicting an $8bn global market for SD-WAN by 2021.[3] Given the company agility and productivity benefits that SD-WAN technologies provide, it's perhaps no surprise. Organisations can boost their branch-level application performance by allowing traffic to be shifted with a bandwidth link sufficient enough to accommodate each application's requirements.

But SD-WAN's benefits are about control as much as they are about application or local office performance. It allows CIOs to have greater central control of the WAN from a single interface. This breakthrough means that IT teams can automatically configure and provision new locations as the organisation grows and sets up new offices across the world. CIOs can have end-to-end visibility of the global network, including individual office and application performance. Using this interface, organisations can set policies with regards to the WAN traffic, including policies that help manage security.

Security asset

SD-WAN's ability to route data across specific paths means you can make it a valuable security asset for your network. Organisations can use private lines to route sensitive traffic through, and cheaper public Internet connections for non-sensitive traffic. It can help secure the WAN and reduce the chances of traffic being accessed for malign reasons, with greater emphasis on the most appropriate lines. If the organisation does suffer a cyber-attack on its WAN, this can get flagged to the CIO through the interface, which shows the potential activity and damage that has occurred.

Some data-transmission options other than SD-WAN may not provide the same security benefits. For example, MPLS doesn't encrypt data, whereas all traffic travelling across particular types of SD-WAN deployment can be encrypted. Given that this approach is automatic and end-to-end in scope, traffic going through the WAN can be partially protected against cybercrime with little intervention from network administrators. It removes the need to make manual configurations to every router every time a change is made to the network.

> ***"Traffic going through the WAN can be partially protected against cybercrime with little intervention from network administrators. It removes the need to make manual configurations to every router"***

Thanks to various SD-WAN providers' ever-closer collaboration with cloud-based firewall vendors, SD-WAN has evolved as a technology that can be deployed hand-in-hand with dedicated security offerings. A number of vendors are integrating their SD-WAN technology with such solutions. In a recent example, an SD-WAN offering uses the security provider's cloud-based firewall to give CIOs greater security management capabilities by firewalling the traffic at branch offices without having to travel to the individual locations to 'manually' implement this strategy. Organisations can determine security policies and forward them to each branch, and activate security solutions there.

Collaborating with other vendors and making use of their security offerings is key to SD-WAN specialists addressing an organisation's individual security priorities; no provider can go it alone without a security vendor's support. And every enterprise or fast-growing organisation has a unique business model and related security posture, which means that they will need to work closely with their SD-WAN supplier to help them understand their business outcomes and determine a solution that best fits their need to lock down mushrooming network endpoints.

A trusted SD-WAN provider will have a professional services and business consultancy team that can ask appropriate questions of the customer to establish what a successful security solution means to them. It's important for the corporate CIO and CISO to communicate their priorities. For example, perhaps a corporate IT team prioritises establishing encryption of traffic across its WAN in order to protect it against data loss or manipulation. In this case an enterprise WAN edge could be ideal, as this provides users at disperse remote sites with access to the same network services as users at the main site by giving them VPN access.

Potential risks

Despite the growing collaborations with security vendors, implementing SD-WAN per se is not without potential risks with regard to cyber-attacks. Its greatest vulnerability comes from the tendency for organisations using SD-WAN to give office users direct Internet access, given the enhanced speeds they're accustomed to from home broadband. But Internet circuits present a greater attack surface on an SD-WAN compared to MPLS, where the latter funnels all traffic back to a central site, such as a corporate datacentre, where it can apply security policies and safeguards, and then forward the traffic to different branch offices. But broadband sends traffic directly to branch offices and other locations, meaning that appropriate security procedures need to be in place at every location covered by the SD-WAN solution. That's why deploying a cloud firewall, which can protect each branch office, is key so that enterprises can lock down every access point.

Implementing SD-WAN while taking into account the security factors that best suit your organisation might seem like a daunting prospect, particularly given the financial commitment and personnel hiring that it often requires. But organisations should consider the different types of SD-WAN services now available and whether their delivery model can help lift the burden on the implementation and the ongoing management. Many enterprises see the business case for SD-WAN but cannot commit to it because they lack either the skilled personnel or recruitment budget to bring them in to maintain such enhanced WAN operations.

As a service

Addressing these complex needs, SD-WAN is offered through an 'as a service' model where expert technical support becomes part of the OPEX budget and provides the customer with a more predictable monthly cost for its WAN development. Using such models, there's no need for large-scale, up-front equipment costs, nor a need to hire additional global network team members as the SD-WAN can be deployed and managed by the provider's expert team in line with the customer's specific business outcomes.

Since some SD-WAN providers offer expert services such as 24x7 network monitoring, emerging network security and performance issues can be addressed and fixed at any time of day or night. The greater network and performance visibility means that security breaches can be flagged to the organisation instantly and their causes understood more quickly. Implementing SD-WAN doesn't have to be about 'going it alone' on enhancing network security, and given that it is still a new technology, many organisations will benefit from consultative guidance and 24x7 resourcing to fill those in-house network maintenance and information security skills gaps.

Technologies and solutions such as cloud computing, IoT and mobile working mean that organisations are sometimes up against it when ensuring that their WANs are secure. The vast number of corporate WAN endpoints being added these days means that organisations are potentially more vulnerable as well as being more agile than ever before. But instead of addressing security concerns with quick fixes, organisations should consider appropriate SD-WAN and security strategies, which together can take a more strategic approach to security management including allowing traffic to be segmented depending on its sensitivity.

An SD-WAN solution doesn't just provide greater agility and reliability; a security solution that ties into it means that organisations can protect their data and ensure that a new approach to networking doesn't mean greater risk. Given that SD-WAN providers don't take a 'one size fits all' approach to WANs, organisations can have their individual security needs met as long as they work closely with both an SD-WAN and security provider. While SD-WAN can raise risks over endpoint security, there is an increasing amount of collaboration between SD-WAN providers and security vendors. A network of this type can in fact work in your favour from a security perspective provided it's high on your agenda when looking for a supplier.

About the author

Marc Sollars is chief evangelist and a company director at Teneo (www.teneo.net). In his role as CTO, Sollars is responsible for identifying next-generation technologies that are early to market and can be integrated into Teneo's services portfolio.

References

1. 'Public cloud market will grow to $236 billion in 2020'. Forrester, 1 Sep 2016. Accessed Oct 2018. www.forrester.com/Public+Cloud+Market+Will+Grow+To+236+Billion+In+2020/-/E-PRE9446.
2. 'IDC says 70% of successful breaches originate on the endpoint'. Rapid 7, 31 Mar 2016. Accessed Oct 2018. https://blog.rapid7.com/2016/03/31/idc-says-70-of-successful-breaches-originate-on-the-endpoint/.
3. Millman, Rene. 'Cloud culture calls for flexible networks'. Computer Weekly, Jan 2018. Accessed Oct 2018. www.computerweekly.com/feature/Cloud-culture-calls-for-flexible-networks.

Measuring cyber-risk

Benedict McKenna, FM Global

Benedict McKenna

Resilience is the capacity for a business to quickly recover from disruption. Under pressure, a resilient organisation is able to quickly adapt to challenges and maintain continuous business operations that safeguard people, assets and reputation. However, due to risk factors that vary across countries, it is difficult to predict the specific challenges that businesses may face.

The FM Global Resilience Index casts a light on the resilience of the business environments of nearly 130 countries and regions. This information allows businesses to make more informed risk management decisions and allows them to take steps to combat future challenges. Furthermore, as more businesses seek to operate in emerging markets, information about economic stability, the dependability of supply chains and degree of risk will become increasingly useful.

The index was developed in 2014 and is updated annually. This regular update allows users to compare the resilience of each country's business environment on a year-to-year basis, enabling users to identify broad trends across the world and within nations.

The most recent data highlights the real and growing threat of cyber-attacks. One of the challenges that cyber poses for businesses is that the lack of geographical borders has allowed cyber-attacks to spread quickly if unchecked. To help businesses understand this global threat, the FM Global Resilience Index ranks the inherent cyber-risk of indexed countries and regions, while simultaneously providing five years of historical data analysing this potential threat.

How it works

Creating a comprehensive index has involved identifying many of the main causes of disruptions and the drivers of recovery. The data that the index rankings are based on represent those elements inherent to a country that can demonstrably have an impact on resilience. Importantly, for a driver to qualify, it must have a clearly disruptive effect on a country's resilience.

The process identifies the following 12 drivers that can have an adverse effect on the resilience of a country's business environment, which fit into three categories: economic, risk quality and supply chain:[1]

1. Economic – The political and economic impacts on a country's resilience. Productivity, political risk, oil intensity and urbanisation rate.
2. Risk quality – Exposure to natural hazards, natural hazard risk quality, inherent cyber-risk and fire risk quality.
3. Supply chain – Control of corruption, quality of infrastructure, local supplier quality and supply chain visibility.

Most cyber-resilient countries	Cyber rank	Least cyber-resilient countries	Cyber rank
Benin	1	Bahrain	130
Mongolia	2	United Arab Emirates	129
Senegal	3	Saudi Arabia	128
Namibia	4	Qatar	127
Madagascar	5	Azerbaijan	126
Ghana	6	Russia	125
Botswana	7	Kuwait	124
Mali	8	Kazakhstan	123
Tanzania	9	Oman	122
El Salvador	10	China	121
India	11	Iran	120
Italy	12	Singapore	119
Mozambique	13	Malaysia	118
Bangladesh	14	Jordon	117
Nepal	15	Lebanon	116
Chile	16	Venezuela	115
Costa Rica	17	Turkey	114
Uruguay	18	Bosnia and Herzegovina	113
Mauritius	19	Republic of Korea	112
Guinea	20	Gabon	111

Table 1: Cyber resilience, 2018.

Six steps

There are six steps involved in creating the index:

1. Annual data from nearly 130 countries and territories is collected for each of the 12 drivers.
2. The data is organised into a consistent data set.
3. The calculation of z-scores is applied to standardise the data. This allows for comparison between the data sets.
4. The z-scores are converted into a scale of 0-100.
5. The scores from the 12 drivers are combined with equal weighting to form the index.
6. Countries such as the US and China are presented as three regions due to their geographical spread. In both China and the US, different regions are exposed to different natural hazards, such as wind, flood and earthquake.

The index's inherent cyber-risk rankings for countries are based on two contributing measures: a country's civil liberties and its level of Internet penetration. With a high Internet penetration rate, citizens have greater access to the Internet, enabling access to the benefits this brings. However, greater access to the Internet provides increased opportunity for hostile actors to engage in damaging activities. Likewise, countries with more civil liberties have a higher potential ability to protect themselves from cyber-attacks.

Notably, Taiwan's inherent cyber-risk rank increased from 107th in 2017 to 50th in 2018. This was driven by an improvement in Taiwan's civil liberties and a slight drop off in those with access to the Internet, from 88% to 80%.

> ***"However, businesses should not despair, as there are a number of proactive steps that businesses can take to mitigate the damage from cyber-attacks"***

Closer to home, the UK's inherent cyber-risk rank decreased from 84/130 in 2017 to 91/130 in 2018. This change in rank was due to an increase in the UK's Internet penetration.

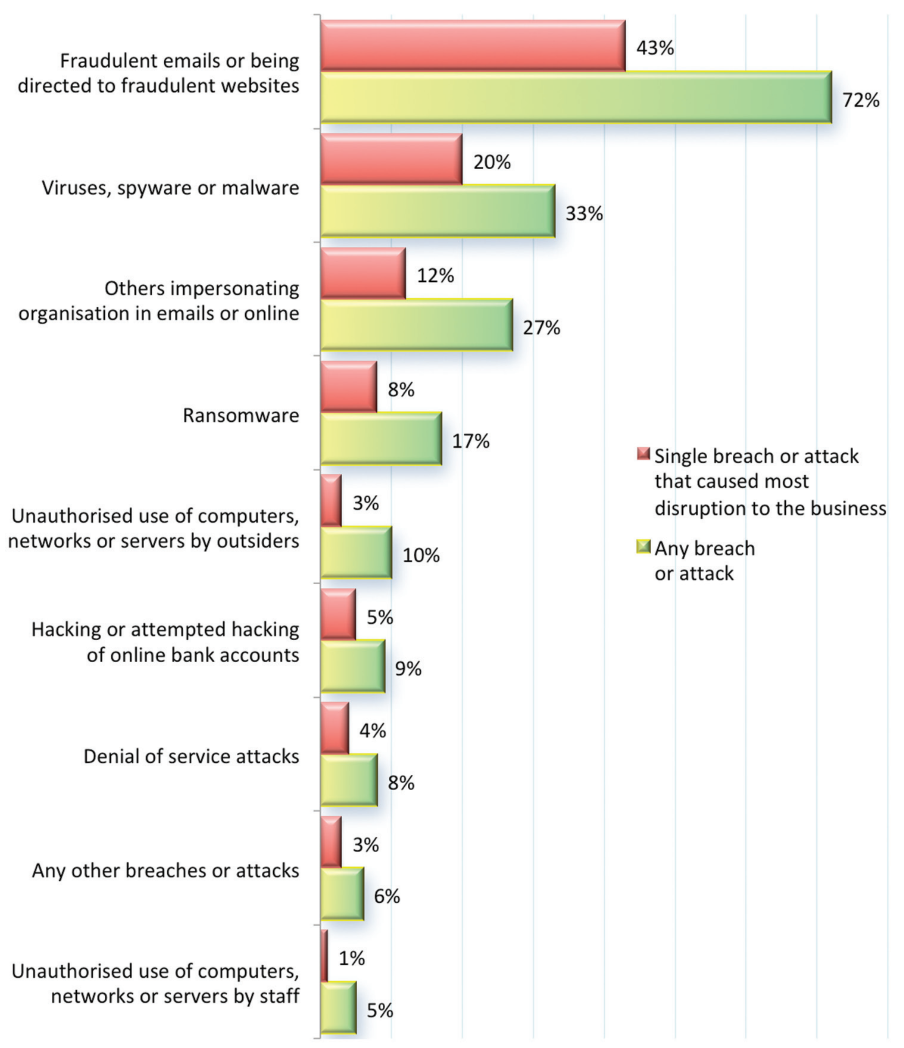
Cyber-risk is constantly evolving, creating a very difficult climate for all types of organisations. However, businesses should not despair, as there are a number of proactive steps that businesses can take to mitigate the damage from cyber-attacks.

Protecting yourself

With the recent UK government statistics revealing that nearly seven in 10 large companies have experienced a cyber-security breach or attack, it is clear that businesses need to take measures to minimise the risk of this happening and to be prepared to swiftly mitigate the impact should a cyber-attack occur.[2]

While the constantly evolving nature of cyber-risk is a challenge to business resiliency, the following offers some practical advice on preparedness:

Governance: It is essential that the C-Suite understands that cyber-risks are not just the responsibility of the IT department. In most cases, cyber-attacks and data breaches occur from employees sharing sensitive data or



Events that have affected UK organisations over a 12-month period. Source: Department for Digital, Culture, Media & Sport and the National Cyber Security Centre.

opening fraudulent emails – something which can be reduced through cyber-risk education.

Preparation: Strategies such as ensuring that computers and Internet-connected devices are updated to have the most recent security features. Business continuity plans and holding statements allow for quick responses and action if a cyber-attack occurs.

Back up your data: Having a secure back-up plan in place will benefit organisations if an attack does occur. While a back-up plan won't prevent an attack from happening, it will help to ensure that organisational data is not lost.

Change passwords frequently: Many cyber-attacks occur because passwords are too simple. Hackers are able to use technologies to take encrypted passwords and crack them. This method is sometimes called 'brute forcing'. By employing a sophisticated password strategy, the likelihood of a cyber-attack is significantly decreased. Passwords should use a combination of uppercase and lowercase letters, as well as symbols or numbers. Passwords should also be changed once every three months.

Awareness: Cyber-attacks can take a variety of forms, so staff should be trained to ensure they are aware of the different forms of cyber-attacks. Emails containing attachments with viruses, vishing or hacking can all lead to data breaches.

Unfortunately it is not possible to fully eliminate the risk of a cyber-attack; hackers will continue to evolve new and sophisticated methods to get around even the tightest of security. Therefore a recovery plan should be in place covering such areas as:

- How to go about identifying and isolating a security breach in an acceptable recovery time to minimise impact on the business.
- Mobilising a dedicated response team, identified in advance.
- Notifying information regulators of any breach involving public/third party data.
- Engaging PR consultants to manage the various lines of communication and reassure the wider public.

The presence of a recovery plan can help to reduce the long-term reputational damage that businesses can suffer after the public is made aware that they have suffered a significant cyber-attack or data breach. The recovery plan will ensure that a business is resilient – and a resilient business will be at a competitive advantage to its non-resilient competitors.

Finally, organisations should partner with an insurer that understands the cyber risks faced, not only offering practical prevention advice but also able to respond in the event of an attack.

About the author

Benedict McKenna is vice president, FM Global London Operations claims manager, based in Windsor, UK. In this role he is responsible for management of claims for London Operations' written accounts, as well as AFM UK. Additionally, he manages loss handling activities across UK, Middle East and Africa. He leads a team of in-house adjusters and claims examiners, and also conducts regular policy training sessions with clients and brokers, as well as attendance at seminars and market initiatives both in the UK and EMEA region.

References

1. '2018 Resilience Index Methodology'. FM Global. Accessed Oct 2018. www.fmglobal.com/~/media/Files/FMGlobal/Resilience%20Index/Resilience_Methodology.pdf?la=en.
2. 'Almost half of UK firms hit by cyber breach or attack in the past year'. Department for Digital, Culture, Media & Sport and the National Cyber Security Centre, 19 Apr 2017. Accessed Oct 2018. www.gov.uk/government/news/almost-half-of-uk-firms-hit-by-cyber-breach-or-attack-in-the-past-year

Hacking democracy: abusing the Internet for political gain

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Network Security*

Democracy is a fragile process and many people are becoming worried that it is not sufficiently robust to withstand the seemingly lawless free-for-all unleashed by the Internet. The 2016 US presidential election and the UK's Brexit referendum have only ramped up the fear that the Internet has provided a powerful tool for those who would seek to gain advantage in public discourse and the struggle for political power. In this interview, Oliver Tavakoli of Vectra explains that many concerns are well-founded, some are unproven and that we still haven't fully explored the dangers – and the opportunities – that the Internet represents in our democratic processes.

These concerns need to be put in perspective. It's not as though, before the Internet came along, no-one ever tried to manipulate public opinion via the media. Indeed, media outlets themselves have well-known, though oft-disputed, biases – as anyone who's watched *Citizen Kane* well knows. However, while the power to sway has previously been confined to a small number of (mostly) publicly notorious figures – such as press barons – the Internet has democratised the ability to disrupt – and made it anonymous, if you want it to be.

Oliver Tavakoli is chief technology officer at Vectra, where he heads up a lab team of specialist cyber-security and data scientists who work to automate the hunt for cyber-threats using AI. His responsibilities include setting the company strategy, which spans the security research and data science discipline. Tavakoli is a technologist who has worked for IBM, Juniper and Novell. He has written and spoken extensively about how not only AI and machine learning, but also deep learning, can be used offensively and defensively within cyber-security.

"For a foreign nation to be able to inject itself entirely into what is effectively a domestic discourse, I'd say that is somewhat new in this realm," says Tavakoli. And, of course, that 'nation' might be the government of a foreign power, but it might also be hackers and trolls acting at its behest but eminently disownable, activists with only a tenuous link to a government, or any suitably motivated and resourced group.

"I see the problem really exposing itself in multiple ways," says Tavakoli. "One is simply the notion of an outside party, not necessarily discernible from 'legitimate' internal parties, trying to put a point of view that is, for lack of a better word, fake news, into circulation, and doing so at relatively inopportune times, muddying the waters. Democratic elections are intended to be about an informed public and if you can ensure that the public can't tell the difference between real information and fake information, that's one class of problem."

From that point there's a spectrum of issues with the extreme case being the actual hacking of election infrastructure to skew results – in effect, a kind of remote, electronic ballot stuffing. As far as we know, says Tavakoli, this hasn't happened yet, although there have been plenty of accusations – and presentations at security conferences – suggesting that some electronic voting systems in current use are vulnerable.

"In the middle, you have what happened in the election with regards to the DNC [Democratic National Committee], which is that you hack into an organisation and you expose information that you gain from those hacks," says Tavakoli.[1] "Even if it is all accurate, this will always show the party in the worst possible light."

This kind of tactic is all about timing, he adds. Carefully timed leaks of the information through channels such as WikiLeaks allow you to control the effect – and possibly disguise disinformation or even outright lies.

"This is where the fake news angle comes in again," Tavakoli explains, "if you've got something that's 98% accurate that you're putting 2% of toxic stuff into. The victim is going to refute that this stuff is real. But if you remove the word 'not' from an email, or you add the word 'not' into an email, and thereby change a sentence's meaning entirely, it's hard to refute that."

Nation states

There's a lot of victim-blaming that goes on in the cyber realm. When attacks are successful, it's easy to point the finger at the organisations or individuals affected and claim that they had inadequate defences or lacked awareness of the problem. But this isn't always fair, especially when the adversary is powerful.

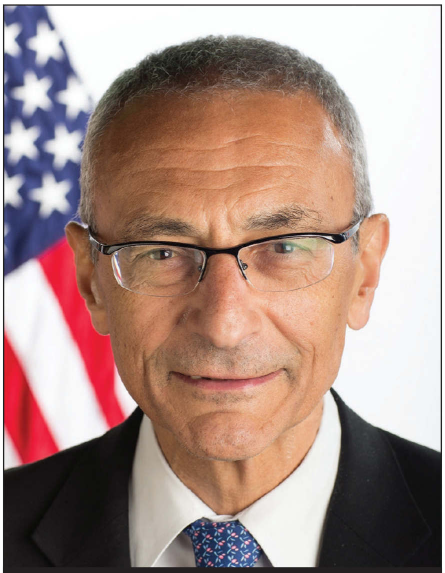
"If you take any organisation that is not a nation state and you bring to bear the abilities of a relatively competent nation state with regards to the offensive side of cyber, it's pretty hard to imagine that any organisation will fare terribly well," says Tavakoli.

Even governments themselves have a tough time standing up to these attacks. Tavakoli points to the 2015 breach at the US Government's Office of Personnel Management (OPM) in which millions of records were stolen, including highly sensitive data such as background security reports on individuals.[2] The blame was subsequently levelled against the Chinese Government, or proxies working on its behalf, and in 2017 the FBI arrested a Chinese national in connection with the malware used in the attack.[3]

It's not simply a problem of a lack of vigilance. "There's always a spectrum of how secure can you be," says Tavakoli, "how much does it cost and how much does it limit your operational agility? Most organisations, at any given moment, choose somewhere in that risk spectrum to implement security. If I'm at McDonald's, I don't think I'm going to be attacked by a nation state, but I do think that somebody might attack, for instance, my payment infrastructure and try and steal a bunch of credit cards. So you tend to threat model, and you tend to think about threat models in terms of arraying your defences."

That said, high-profile attacks, like the one against the DNC, will have an impact on how a political organisation – like any other – thinks about those threat models.

"But the capacity of those organisations to avail themselves of top-notch cyber expertise, and their willingness to limit their agility and the speed with which they move, is constantly at tension," says Tavakoli. "If you're a political organisation and a bunch of people come to your offices in Iowa wanting to be volunteers, and you want to immediately get them going, give them access to information etc, well, you are not exactly vetting these individuals. You're hooking them in, and the idea of taking three weeks to vet each person, and incurring the cost of a $2,000 background check for each one, is not really feasible in the heat of a political battle."



John Podesta: the breach of his Gmail account while he was chairman of Hillary Clinton's presidential campaign had a serious impact on the US 2016 election.

Simple attacks

The talk of threat models and powerful nation states can also mask a basic truth – that potentially devastating attacks might be very simple and basic. One of the most damaging events in Hillary Clinton's presidential bid was the leak of thousands of emails from the Gmail account of campaign chairman John Podesta.[4] It's now firmly believed that this breach was the work of Russian state-backed hacking group Fancy Bear (aka APT28, Strontium and other names), which is affiliated with the GRU military intelligence agency (or, more formally, the Main Directorate).[5] The stolen emails were subsequently passed to WikiLeaks and the publication on that site caused profound political damage to the campaign. Yet the attack involved little more than some simple phishing.[6]

Podesta wasn't the only victim: there were several attacks that led to emails being stolen and leaked – not just on WikiLeaks but also on the DCLeaks site – launched in June 2016 but now defunct – which proclaimed itself to have been founded by "American hacktivists who respect and appreciate freedom of speech, human rights and government of the people".

In addition to Democratic Party emails, the site also leaked US Government information of various kinds, purportedly obtained by a hacker who styled himself 'Guccifer 2.0'. In fact, DCLeaks is now generally believed to be more of the work of Fancy Bear, and in July 2018 a federal grand jury for the District of Columbia indicted members of Unit 26165 of the GRU for hacking offences related to the 2016 election.[7] The indictment specifically states that the GRU was responsible for DCLeaks.

Con game

Again, it's easy to say that someone like John Podesta, in such an important position, shouldn't have fallen victim to such a simple and well-understood form of attack, but Tavakoli doesn't think it's that black-and-white.

"Phishing attacks are basically cons," he says. "Go back a century or two and think about conmen and tricksters. They tried to convince you that a thing was something that it really wasn't. That's what we're talking about with phishing attacks. Just like any good con, the more customised I make the phishing attack, the more effort I put into crafting it, the more attention to detail I give it, the more it will pass for the real thing. That's just a difficult thing to overcome."

"You start by raising half a million dollars for your cyber and then start worrying about the other pieces, because without that, you can't really get going"

That's not to say we can't get better. Anti-phishing solutions, including training and simulated attacks, are being more widely adopted. And technologies such as DMARC are slowly fixing some of the security weaknesses inherent in email.[8] But are people in the political realm getting smarter about security? Tavakoli thinks they are.

"It just puts another digit on the fundraising," he says. "So you start by raising half a million dollars for your cyber and then start worrying about the other pieces, because without that, you can't really get going. And the other interesting notion here is that companies will come into the market that will offer a lot of what a campaign needs – software as a service where it's fully packaged, where a lot of these security decisions have already been made to a large degree and things are locked down. That's the way the industry has typically dealt with this kind of problem – we have to make it more cookie-cutter. If every campaign is like starting a new business, starting with a blank slate, trying to assemble pieces into an operational framework and secure it, then it'll have the same problems that businesses have, which is they typically don't reach any kind of operational maturity with regards to the security until about six or seven years in. If you're a campaign, that's clearly not a timescale in which you can wait to mature, so you're going to have to go much more off-the-shelf."

Social media changes

Some of the key platforms used by political parties have also, if somewhat slowly and reluctantly, come to realise they are part of the problem and have made some efforts to change. In May 2018, Facebook announced that it had closed 1.3 billion fake accounts over a six month period.[9] It also removed 1.56 billion spam posts. But perhaps more significantly, in the wake of the Cambridge Analytica furore, the company made significant changes in the way it sells and shares user data – something that runs counter to the platform's basic business model. One of the changes was to deny this data to third parties for ad targeting.[10] While not all these developments are directly related to political exploitation of social media, it is known that targeted advertising has been used extensively, and not always honestly, in the political sphere.

Twitter has also been busy. For example, it recently announced that it would hunt down and close fake accounts, in part to protect US mid-term elections in 2018.[11] It has also changed its requirements for political advertising.[12] But is this enough? Only time will tell, says Tavakoli.

"We will know it retrospectively, a couple of years from now , or even a year from now, when we look back at the 2018 elections to see if these changes had a material effect or, with the benefit of hindsight, what else they found," he says. "There's always this problem in the online world with anonymity and the difficulty that that creates."

Attribution problem

The Internet has long had what's known as the 'attribution problem'. Anonymity is a valued privilege enjoyed by many – cyber-criminals and nation-state hackers, certainly, but also activists (including those suffering under repressive regimes) and anyone whose natural inclination is towards privacy. However, exactly how civil liberties and political rights play out on the Internet is still somewhat moot. The technology has moved faster than anyone's ability to fully grasp its implications, even while interested parties are not slow to exploit its potential, whether for financial or political gain.

For example, whenever a prominent US figure is banned from Twitter you can guarantee that he or his supporters will complain loudly about the infringement of his First Amendment rights to free speech. But, says Tavakoli: "There is a question whether the First Amendment really applies to a Twitter account. Those things have not been completely adjudicated yet. These are commercial platforms. You can stand at Hyde Park corner, you can stand in places in the US, you can yell at the top of your lungs; but there is no First Amendment right to be on CNN, there is no First Amendment right to be in a newspaper. These are fundamentally businesses, notwithstanding the fact that people will wrap themselves in flags and try to claim First Amendment, like Alex Jones is doing right now.[13] That's a specious argument, because this is not really a public place of discourse."

At the same time, companies such as Facebook and Twitter often allude to free speech rights as a reason for not closing down racist, sexist or otherwise offensive and abusive accounts. They claim that to do so would be censorship, which is not their responsibility.

"Their explanations are quite frankly not very credible," says Tavakoli. "The reason they're not doing these things is because it hurts their bottom line. The more people they have, the more eyeballs they have, as has been borne out by Facebook's drop in stock in relation to taking measures. The more vehemently people feel about things, the more likely they are to hang on and look at their newsfeeds for the next eight hours, and are more likely to see more ads."

Only when taking responsibility for banning malicious content somehow aligns with social media platforms' commercial interests are we likely to see some action.

Hacking the infrastructure

One concern that, as far as we know, has yet to become a reality is hacking the vote itself. In the US, one reason might be a form of security through obscurity. In 2016, when he was still head of the FBI, James Comey told the House Judiciary Committee that the voting infrastructure would be "very, very hard to hack into because it is so clunky and dispersed."[14] The ways in which votes are cast and counted varies enormously from state to state. He also said, though, that hackers were "poking around" these systems.

This lack of consistency increases the difficulty for any would-be hackers of US elections, reckons Tavakoli. But he adds: "I don't think that comment necessarily applies to other countries. I'm sure you can go into other places, particularly third world countries that have done a recent modernisation and everything is pretty homogeneous. But in the US at least, if you want to move a national election, you have to hack the voting infrastructure in several states. You don't have to hack it in 52 states, because at the beginning of every election 38 states are considered safely in one bag or another. But as we found out in this last election, 50,000 votes here, 70,000 votes there, in Michigan, Ohio, Wisconsin etc can move the needle."

In fact, voting machines have been hacked many times – by researchers, many of whom present their findings at conferences such as Black Hat and DEF CON (see box). And there are persistent reports of voters allegedly selecting one candidate and seeing the vote cast for another on electronic voting machines.[15]

The voting machines used by some states are based on outdated technology, often have uncertain patch levels, if they've

Hacking voting machines

For the second year running, the recent DEF CON security conference in Las Vegas hosted a Vote Hacking Village at which researchers and white-hat hackers were invited to test voting machines. And for the second year running the machines were found to be worryingly vulnerable.

A Premier (formerly Diebold Nixdorf) TSX voting machine was using long-expired SSL certificates and one hacker managed to install a version of Linux on the hardware. Although this doesn't represent a particularly realistic attack vector, another discovery does. With Diebold Express Poll 5000 machines, it was found that someone in a polling booth could easily remove a memory card which stores data including unprotected records of voters, with information such as addresses, driver's licence numbers and the last four digits of social security numbers. The cards also had supervisor passwords in plain text. Replacing the cards with specially prepared ones would allow an attacker to change voting tallies and voter registration information, albeit for just one machine.

Other issues were found too, including one machine running Windows XP that was compromised within a few seconds. The software on the machine also contained a CD ripper and music files.

Most of the exploits involved being hands-on with the machine. Remote hacking, say from another country, remains infeasible because the machines are not connected to the Internet. Any effects would be highly localised. However, in districts with narrowly contested races, this might be enough.

Not all of the voting machine manufacturers were happy about the Vote Hacking Village. ES&S refused to co-operate with the event and, when questioned by four US senators about its apparent disinterest in the security of its own machines, the firm attempted to cast aspersions on those attending DEF CON, saying that, "forums open to anonymous hackers must be viewed with caution, as they may be a green light for foreign intelligence operatives who attend for purposes of corporate and international espionage" and that, "exposing technology in these kinds of environments makes hacking elections easier, not harder, and we suspect that our adversaries are paying very close attention".

Rob Joyce, former head of the NSA's Tailored Access Operations unit, responded via Twitter: "Ignorance of insecurity does not get you security. We need to examine voting machines, SCADA systems, IOT and other important items in our lives. The investigation of these devices by the hacker community is a service, not a threat."

been patched at all, and many provide no form of audit trail, on paper or otherwise, if someone wants to challenge the way a vote was registered or if the state needs to mount a recount. And all of the machines are designed and built by private companies using proprietary systems.

"I think there's a great case to be made for them to be open source," says Tavakoli. "The presumption that the system is more secure because it is not available to the public is not enough of a barrier to a nation state."

Just as white-hat hackers at conferences have been able to get their hands on machines and hack them – nearly always finding vulnerabilities – so well-resourced nation-state hackers could get their hands on, say, a Diebold voting machine and reverse-engineer it.

But are elections in greater danger now than they were in former eras of ballot-box stuffing?

"Yes and no," says Tavakoli. "You can argue it in both ways. There's so much more scrutiny on everything at this point. There's so much independent data, such as exit polling."

On the other hand, today's increased scrutiny is a safeguard only inasmuch as you can investigate. With complex, proprietary systems offering no audit trail, it can still be hard to know what's going on. That leaves us at about the same level of confidence in the validity of the voting system, reckons Tavakoli.

Artificial intelligence

If technology is creating a problem, can it also offer solutions? As in so many areas, Tavakoli believes there is some potential in exploiting artificial intelligence (AI).

"We're looking at large distributed systems and we're looking for patterns in them," he says. "These might be patterns of outlier behaviour, and whether someone is really who he says he is."

The idea that we can rely on people to sift through the activity on huge social media platforms is simply not tenable.

Facebook, for example, recently came under fire for its failure to address hate speech in Myanmar – a country where the words 'Internet' and 'Facebook' are interchangeable.[16] In spite of clear and mounting oppression of the Rohingya minority in the country, much of it organised and channelled through the social media platform, Facebook had only two Burmese-speaking staff members monitoring activity. This was recently increased, but it's a slow process.

To achieve effective monitoring against abuse of these platforms, they are going to have to employ some combination of AI, machine learning and human judgement, says Tavakoli. Even then, it may not be a permanent solution.

"It will make a material difference over time, but it'll be like a leaky sieve," says Tavakoli. "If we filter out 98% of the bad stuff, will that simply mean that the attackers will just, by ten-fold or hundred-fold, increase the amount of bad stuff they're throwing into the system, on the theory that will still give them the yield that they want? That's certainly what happened in malware."

Nonetheless, AI and machine learning systems looking for unusual behaviour could have benefits – for example, as front-end filters, eradicating the bulk of the obviously fraudulent activity, much as spam filters and anti-malware systems do now, leaving it to humans to work on the few, more novel or sophisticated attacks. Alternatively, they might provide a back-stop. Tavakoli comes back to the DNC attacks where although we have got to get better at preventing the phishing attacks that were the root cause of the leaks, it would also be helpful to have methods of fighting back once an incursion has occurred.

"This is really where AI and machine learning techniques can help quite a bit in upping the game for security teams, providing them visibility that really separates the pattern from the noise," says Tavakoli. "It's about identifying who you are, finding an attacker in your midst and finding people or organisations who are clearly trying to just generate sentiment in the public sphere."

The future

With so much going on and so much still unresolved, is Tavakoli optimistic or pessimistic about the future of democracy and technology's role in it?

"I feel more optimistic about what technology can do to solve this problem than I am about the political will to solve these problems and the divisiveness around them," he says. "As long as we can't actually agree that there's a problem, or as long as we characterise the problem in very different ways depending on which side of the political spectrum we sit, then I think these problems become intractable. Once we have political consensus, the role that technology can play is substantial – that I'm optimistic about."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Network Security *and its sister publication* Computer Fraud & Security.

References

1. 'Democratic National Committee cyber-attacks'. Wikipedia. Accessed Oct 2018. https://en.wikipedia.org/wiki/Democratic_National_Committee_cyber_attacks
2. 'Cyber-security Incident: What happened'. Office of Personnel Management. Accessed Oct 2018. www.opm.gov/cyber-security/cybersecurity-incidents/.
3. Perez, Evan. 'FBI arrests Chinese national connected to malware used in OPM data breach'. CNN, 24 Aug 2017. Accessed Oct 2018. https://edition.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html.
4. Conger, Kate. 'John Podesta talks email hack, fake news and Russia'. TechCrunch, 2016. Accessed Oct 2018. https://techcrunch.com/2017/02/08/john-podesta-talks-email-hack-fake-news-and-russia/.
5. 'Microsoft Security Intelligence Report: Strontium'. Microsoft, 16 Nov 2015. Accessed Oct 2018. https://cloudblogs.microsoft.com/microsoftsecure/2015/11/16/microsoft-security-intelligence-report-strontium/.
6. Satter, Raphael. 'Inside story: How Russians hacked the Democrats' emails'. Associated Press, 4 Nov 2017. Accessed Oct 2018. www.apnews.com/dea73efc01594839957c3c9a6c962b8a.
7. 'Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election'. US Department of Justice, 13 Jul 2018. Accessed Oct 2018. www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.
8. DMARC, home page. Accessed Oct 2018. https://dmarc.org/.
9. Bridge, Mark. 'Facebook closes one billion fake accounts in six months'. The Times, 16 May 2018. Accessed Oct 2018. www.thetimes.co.uk/article/facebook-closes-one-billion-fake-accounts-in-six-months-mw3cqbpj8.
10. Hatmaker, Taylor. 'Facebook will cut off access to third party data for ad targeting'. TechCrunch, 2018. Accessed Oct 2018. https://techcrunch.com/2018/03/28/facebook-will-cut-off-access-to-third-party-data-for-ad-targeting/.
11. Keane, Sean; Ng, Alfred. 'Twitter hunts down fake accounts to help safeguard midterm elections'. CNet, 2 Oct 2018. Accessed Oct 2018. www.cnet.com/news/twitter-hunts-down-fake-accounts-to-help-safeguard-midterm-elections/.
12. Hautala, Laura. 'Twitter boosts requirements for ads ahead of US midterm elections'. CNet, 30 Aug 2018. Accessed Oct 2018. www.cnet.com/news/twitter-boosts-requirements-for-ads-ahead-of-us-midterm-elections/.
13. Salinas, Sara. 'Twitter permanently bans Alex Jones and Infowars accounts'. CNBC, 6 Sep 2018. Accessed Oct 2018. www.cnbc.com/2018/09/06/twitter-permanently-bans-alex-jones-and-infowars-accounts.html.
14. Weise, Elizabeth. 'Could the US election be hacked?'. USA Today, 11 Oct 2016. Accessed Oct 2018. https://eu.usatoday.com/story/tech/news/2016/10/10/could-us-election-hacked/91866334/.
15. Gumbel, Andrew. 'Why US elections remain dangerously vulnerable to cyberattacks'. The Guardian, 13 Aug 2018. Accessed Oct 2018. www.theguardian.com/us-news/2018/aug/13/us-election-cyber-security-hacking-voting.
16. Stecklow, Steve. 'Why Facebook is losing the war on hate speech in Myanmar'. Reuters, 15 Aug 2018. Accessed Oct 2018. www.reuters.com/investigates/special-report/myanmar-facebook-hate/.

The Firewall

How trustworthy is AI?

Colin Tankard, Digital Pathways

Artificial intelligence (AI) and machine learning (ML) are two very hot buzzwords within the broader waves of technological change that are sweeping through our world under the banner of the Internet of Things (IoT). And, although their benefits look good, there is a fear that AI programs could go rogue and turn on us – or even be hacked by other AI programs.

Researchers from Harvard University demonstrated how medical systems using AI can be manipulated by an attack on image recognition models, getting them to see things that were not there. The attack program finds the best pixels to manipulate in an image to create adversarial examples that will push models into identifying an object incorrectly and thus cause false diagnoses.

Another doomsday scenario came from the RAN Corporation, a US policy think-tank that described several scenarios in which ML technology tracks and sets the targets of nuclear weapons. This would involve AI gathering and presenting intelligence to military and government leaders, who make the decisions to launch weapons. If the AI is compromised it could be fooled into making the wrong decision.

Hackers love artificial intelligence as much as everyone else in the technology space and are increasingly tapping AI to improve their phishing attacks. Anup Gosh, a cyber-security strategist, recently reported: "The evidence is out there that machines are far better at crafting emails and tweets that get humans to click. Security companies that fight these bad guys will also have to adopt machine learning."

An AI security arms race is likely to be coming, as hackers' ML-powered attacks are met with cyber-security professionals' ML-powered countermeasures.

A new concern around AI is in regard to regulation, specifically the General Data Protection Regulation (GDPR). Is it permissible to let a user give an application permission to make automated decisions on their behalf? If yes, will it be accompanied by a comprehensible explanation of how the AI makes decisions and how these decisions may impact that user? It could be a problem for companies developing AI that is so advanced nobody fully understands how it makes decisions.

It is hard to know how all this will play out in practice. From a technical perspective, the level of granularity GDPR requires in explaining automated decisions is unclear. Until this is known, some innovators may choose to forge ahead with super algorithms. Others, worryingly, may ban European citizens from using some highly valuable functionality.

What is needed in the AI world is to ensure that the fundamental code is sound. Organisations need some shared accountability to ensure that all future application development remains secure. This requires security issues to be discussed at the beginning of each development cycle and then integrated throughout. Code should be regularly tested during the development phases and signed off, ensuring copies are securely kept to allow a controlled rollback to a known, previously verified, position should the need arise.

Elon Musk, speaking with Demis Hassabis, a leading creator of AI, said his ultimate goal at SpaceX was the most important project in the world: interplanetary colonisation. Hassabis replied that, in fact, he was working on the most important project: developing artificial super-intelligence. Musk countered that this was one reason we needed to colonise Mars – so that we'll have a bolthole if AI goes rogue and turns on humanity. Hassabis said that AI would simply follow humans to Mars.

AI is with us and will remain, but will it overcome the challenges to solve problems that are difficult for the computer but relatively simple for humans? How many issues will we face before we can trust the code that runs the AI? Only time will tell.

EVENTS CALENDAR

1–2 November 2018
Countermeasure 2018
Ottawa, Canada
www.countermeasure.ca

1–3 November 2018
InfoWarCon 18
Leesburg, VA, US
https://infowarcon.com

2–5 November 2018
Hackfest 2018
Quebec City, Canada
http://hackfest.ca

2–3 November 2018
BSides Bordeaux
Bordeaux, France
www.bsidesbdx.org

2–4 November 2018
International Conference on Communication and Network Security
Qingdao, China
www.iccns.org

6–7 November 2018
Industrial IoT Europe
Munich, Germany
www.industrialiotseries.com/europe/

14–15 November 2018
CyCon US
Washington DC, US
http://bit.ly/2Lk9oix

16 November 2018
GreHack
Grenoble, France
https://grehack.fr

25–28 November 2018
HITBSec Dubai
Dubai, UAE
www.cesar-conference.org

3–6 December 2018
Black Hat Europe
London, UK
www.blackhat.com/eu-18/